Deutscher Bundestag **Drucksache 19/14029**
19. Wahlperiode 16.10.2019

Antrag

der Abgeordneten Daniela Kluckert, Frank Sitta, Grigorios Aggelidis, Renata Alt, Jens Beeck, Dr. Jens Brandenburg (Rhein-Neckar), Mario Brandenburg, Dr. Marco Buschmann, Hartmut Ebbing, Dr. Marcus Faber, Daniel Föst, Otto Fricke, Thomas Hacker, Katrin Helling-Plahr, Markus Herbrand, Torsten Herbst, Manuel Höferlin, Dr. Christoph Hoffmann, Reinhard Houben, Ulla Ihnen, Olaf in der Beek, Gyde Jensen, Dr. Christian Jung, Dr. Marcel Klinge, Pascal Kober, Dr. Lukas Köhler, Carina Konrad, Konstantin Kuhle, Alexander Graf Lambsdorff, Michael Georg Link, Dr. Martin Neumann, Hagen Reinhold, Bernd Reuther, Christian Sauter, Dr. Wieland Schinnenburg, Matthias Seestern-Pauly, Bettina Stark-Watzinger, Dr. Marie-Agnes Strack-Zimmermann, Benjamin Strasser, Katja Suding, Michael Theurer, Dr. Andrew Ullmann, Gerald Ullrich, Sandra Weeser, Nicole Westig und der Fraktion der FDP

Smart Automotive – Anforderungen an die vernetzte Mobilität im Auto von morgen

Der Bundestag wolle beschließen:

I. Der Deutsche Bundestag stellt fest:

Visionen des automatisierten und vernetzten Fahrens sind so alt wie das Automobil selbst und haben vielfach Eingang in Film und Fernsehen gefunden. Was jedoch zum Ende des 20. Jahrhundert noch ferne Zukunftsmusik war, wird heute Realität. Aktuelle Fahrzeugmodelle verfügen bereits heute über eine Vielzahl von Assistenzsystemen, die dem Fahrer die Steuerung erleichtern. Diese Systeme treffen ihre Entscheidung aufgrund einer Analyse der Fahrzeugumgebung, welche sie mithilfe von im Fahrzeug verbauten Kameras, Radar- bzw. Laserscanner und Ultraschallsensoren anstellen. Die Besonderheit ist dabei, dass die Umgebungsdaten von einem Computer ausgewertet werden, dem nicht für jede erdenkliche Situation eine Lösung einprogrammiert wurde - dies wäre aufgrund der unendlichen Anzahl an Verkehrssituationen nicht praktikabel. Stattdessen trifft ein selbstlernender Algorithmus die Entscheidung, eine Künstliche Intelligenz (KI).

Der Einsatz von KI wird auf dem Weg zu vollständig autonom fahrenden Autos eine wichtige Rolle spielen. Die weitere Entwicklung ist jedoch zu einem hohen Maße davon abhängig, dass ein "intelligentes Auto" mit einer intelligenten Infrastruktur interagieren (Internet of Things, IoT) kann. Notwendig ist, dass sich das Fahrzeug mit seiner Umgebung vernetzen kann. Hierfür bedarf es intelligenter und kooperativer Verkehrsinfrastruktur wie vernetzte Ampeln oder Verkehrszei-

chen. Das fördert nicht nur die Entwicklung autonom fahrender Fahrzeuge, sondern zusätzlich haben die sich aus der Vernetzung der Informationsquellen im Fahrzeug und seiner Umgebung entstehenden Zusammenhänge das Potential, eine bessere und effizientere Steuerung des Verkehrsflusses zu ermöglichen, eine Verbesserung der Verkehrssicherheit herbeizuführen und zu einer Reduzierung von CO2-Ausstößen beizutragen.

Aus der Vernetzung folgen jedoch auch neue Herausforderungen. Das Fahrzeug ist nicht mehr nur länger Datenempfänger, sondern zeitgleich auch Datenerzeuger. Dieser Umstand macht es gegenüber Cyberattacken verwundbar(er), folglich erhöhen sich die Anforderungen im Hinblick auf Sicherheit und Datenschutz. Da Fahrzeuge sicherheitsrelevante Objekte sind, sind diese zudem höher als bei heute schon umfassend vernetzten Geräten wie Smartphones. Die Sicherheit von Nutzern und weiteren Verkehrsteilnehmern sowie die Integrität des Fahrzeugs und des Datennetzwerks haben oberste Priorität.

II. Der Deutsche Bundestag fordert die Bundesregierung im Rahmen der zur Verfügung stehenden Haushaltsmittel auf,:

1. bei der Planung und Umsetzung von Infrastrukturmaßnahmen Belange der Vernetzung zwischen Infrastruktur und Fahrzeug zu berücksichtigen. Erforderlich ist dafür die Beschaffung von intelligenter und kooperativer Verkehrsinfrastruktur (C-ITS), die ihre Nachrichten für eine große Bandbreite von Diensten, in unterschiedlichen Verkehrssituationen und zwischen verschieden Akteuren übertragen. Die Verwendung von C-ITS stellt sicher, dass alle relevanten Informationen unabhängig vom Herkunftsland des Fahrzeugs empfangen werden können.
2. die zukünftige Beschaffung von intelligenter und kooperativer Verkehrsinfrastruktur durch Anpassung der einschlägigen Vergabevorschriften, v.a. des Gesetzes gegen Wettbewerbsbeschränkung (GWB) und der Verordnung über die Vergabe öffentlicher Aufträge (VgV), zu privilegieren.
3. gemeinsam mit Wirtschaft und Industrie sicherzustellen, dass eine Kommunikation zwischen Fahrzeug und Infrastruktur ("Vehicle to Infrastructure", V2I) und der Fahrzeuge untereinander ("Vehicle to Vehicle", V2V) auch in der Praxis gewährleistet ist. Erforderlich dafür ist eine Netzabdeckung mit zellularen Netzen (5G); in Stadtbereichen ist zudem eine Hochgeschwindigkeits-Nahbereichskommunikation durch WiFi-Netze eine sinnvolle Ergänzung.
4. eine Verkehrsleitzentrale damit zu beauftragen, die entstehenden (Verkehrs-) Daten auszuwerten und zu verwerten. Dabei ist eine kurzfristige Verwertung, beispielsweise durch die Weitergabe von Verkehrsmeldungen an die Fahrzeuge, ebenso wie eine langfristige Verwertung durch Anpassung bestehender Verkehrskonzepte vorzusehen.
5. sicherzustellen, dass die Bürgerinnen und Bürger darauf vertrauen können, dass ihre Daten vor unbefugten Drittzugriffen geschützt sind, indem die Kommunikation hohen Sicherheitsstandards unterworfen wird.
6. dafür Sorge zu tragen, dass Hersteller sich verpflichten, sicherheitsrelevante Softwareupdates für die übliche Nutzungsdauer eines Autos bereitzustellen. Die Gewährleistungszeit der IT-Sicherheit muss für den Besitzer des Autos erkennbar sein.

7. sich auf europäischer Ebene dafür einzusetzen, dass eine gemeinsame Sicherheitsstrategie erarbeitet und umgesetzt wird, die auch die Schaffung einer einheitlichen Sicherheitsstruktur zur Folge haben könnte und dafür zu werben, dass die Federführung bei der IT-Sicherheit für die intelligente Verkehrsinfrastruktur bei der EU angesiedelt wird.

Berlin, den 15. Oktober 2019

Christian Lindner und Fraktion